What is claimed is

1. A network encryption system, comprising:

a first network interface, adapted for connection to a protected network;

a second network interface, adapted for connection to an unprotected network;

a processing part, which manages the encryption of information payload to be sent to the unprotected network, and decryption of information payload which are received from the unprotected network, and said processing part includes a microprocessor therein; and

an encryption and decryption system, including a first high-speed crypto system which operates using dedicated hardware components for cryptographic encryption and decryption, and a second, lower speed crypto system, which carries out said cryptographic operations without dedicated hardware components.

2. A system as in claim 1, wherein said first high-speed crypto system uses field programmable gate arrays which are configured to carry out a specific encryption or decryption operation.

3. A system as in claim 1, wherein said first low-speed crypto system includes a first portion using a cryptographic processor, and a second crypto portion using software running on a general-purpose processor.

4. A system as in claim 1, further comprising a key management subsystem, connected to said processing part via a network interface and communicating using a network management protocol, said key management subsystem storing encrypted software keys therein.

5. A system as in claim 4, wherein said key management subsystem and said processing part communicate via Simple Network Management Protocol.

6. A system as in claim 4, wherein said key management subsystem stores at least one private key by encrypting said keys using a password for the encryption.

7. A system as in claim 4, wherein said key management system maintains addresses of other key management systems.

8. A system as in claim 1, wherein said first high-speed crypto system includes at least one card.

9. A system as in claim 8, wherein said high-speed crypto system includes a first card optimized for encryption of SONET frames and a second card optimized for encryption of ATM cells.

10. A system as in claim 4, further comprising a security interlock on said key management subsystem, and a memory erase function which erases said memory when said security interlock is violated.

11. A system as in claim 1, wherein said encryption and decryption system includes a portion which removes a header associated with the network interface, replaces said header with a cryptographic header, processes said message using the cryptographic header, and then generates a new header associated with the network interface.

12. A system, comprising:

a first network interface, adapted for connection to a protected network;

a second network interface, adapted for connection to an unprotected network;

a processing part including a third network interface, said processing part managing encryption of data from said unprotected network and sending said data to said protected network, and managing decryption of data from said protected network and sending said data to said unprotected network in a specified form; and

a key management subsystem, storing encrypted keys therein for use in decryption by said processing part, connected to said processing part by a network protocol and connected to said third network interface.

13. A system as in claim 12, wherein said network protocol of said third network interface is SNMPV3.

14. A system as in claim 12, wherein said unprotected network is a SONET network.

15. A system as in claim 12, wherein said unprotected network is an ATM network.

16. A system as in claim 12, wherein said unprotected network is a Frame Relay network.

17. A system as in claim 12, wherein said unprotected network is a IP network.

18. A system as in claim 12, wherein said processing part includes an encryption and decryption system, including a high-speed crypto system formed of hardware encryption parts, and a lower speed crypto system operating using a crypto processor.

19. A system as in claim 18, wherein said lower speed crypto system includes a first part that operates in software, and a second part that operates using a cryptographic processor.

20. A system as in claim 18, wherein said high-speed crypto system is formed of field programmable gate arrays.

21. A system as in claim 18, wherein said encryption and decryption system operates to remove a header associated with a network protocol of said unprotected

network, and a header associated with cryptographic functions, process a message portion using said header associated with cryptographic functions, and then read generate a header associated with the network protocol.

22. A method, comprising:

connecting to a first network which is a protected network and a second network which is an unprotected network;

encrypting data being sent from said first network to said second network, and decrypting data being sent from said second network to said first network; and

storing and managing at least one signing key in a separate unit from the unit carrying out the encrypting, and communicating with said separate unit, over a separate network from said first and second network.

23. A method as in claim 22, wherein said encrypting comprises removing a header associated with a network protocol of said second network;

obtaining key information from said separate unit, and forming an encryption header based on said key information and associating said encryption header with a message fragment;

encrypting the message fragment, using said encryption header; and

regenerating the header associated with the network protocol.